We owe it to the families of those who were injured and those who died to do our part to get to the bottom of what led up to January 6.

If we want this Capitol to be available for future generations to visit peacefully in a positive way, let's do our part to make sure we get to the bottom and answer that fundamental question.

I yield the floor.

The PRESIDING OFFICER (Mr. BOOKER). The Senator from South Dakota.

THE ECONOMY

Mr. THUNE. Mr. President, inflation is on the rise. Inflation in June was at its highest level in 13 years. Consumers are facing the effects: higher prices.

Americans are facing increases in rent, in their restaurant bills, in their grocery bills, gas prices, and the list goes on.

Want to buy a used car?

Expect to pay a lot more money than you would a year ago.

Inflation happens when the amount of money out there exceeds the supply of products. When that happens, when demand outstrips supply, prices increase. And that is what we are seeing now. It is being aggravated by Democrats' decision this spring to flood the country with unnecessary money.

During times of crisis, there is a place for increased government spending. The money the government invested in COVID vaccines, for example; the forgivable loans provided to small businesses to help them weather the pandemic; and the increased assistance to hospitals and healthcare providers as the crisis escalated.

But crisis spending is for just that, a crisis, or at least it should be. Unfortunately, Democrats have never met a temporary government dollar that they didn't want to keep spending. ''Temporary'' government programs aren't really a thing for my friends across the aisle.

And so as the crisis was waning and our economy was rebounding, Democrats doubled down on the crisis spending and passed a massive COVID relief bill filled with unnecessary handouts; hundreds of billions of dollars for State governments, the majority of whom were doing just fine without it. In fact, many running surpluses. Tens of billions more for schools who had barely made a dent in the billions of dollars they had already been given.

Republicans and at least one liberal economist warned that Democrats' massive spending plan could overstimulate the economy, but Democrats didn't listen. So it is no surprise that the flood of unnecessary government dollars is currently helping to boost inflation.

Here is the kicker, Mr. President. After flooding the economy with unnecessary money, Democrats are now preparing to double down on that strategy. That is right. Despite passing a largely unnecessary $1.9 trillion bill just 4 months ago, Democrats now want to spend an additional $3.5 trillion—$3.5 trillion.

The truth is that number is likely to be even higher, a lot higher. One estimate suggests that the $3.5 trillion is likely to be more like $5 trillion or $5.5 trillion. That is from an independent analysis by the Committee for a Responsible Federal Budget, where President Biden's own Treasury Secretary used to serve on the board. That is an inconceivably large amount of money.

To put that number in perspective, the entire Federal budget for 2019 was less than $4.5 trillion—the entire Federal budget. So Democrats are just casually tossing out a new spending bill that might very well exceed the entire Federal budget in 2019.

I can assure Americans that that much money would fuel increased inflation. Consumers would continue to be squeezed by rising prices and watch the value of their salaries decrease.

But the damage would not be just limited to the effects of inflation. Americans would also suffer as a result of the massive tax hikes Democrats are envisioning. Democrats plan to pay for all or some of their spending by raising taxes left and right on small businesses, large businesses, investment, well-off Americans. All of them and more will see tax increases under Democrats' plans.

The President, of course, likes to repeat his mantra that he won't raise taxes on those making under $400,000. In fact, that isn't really true, as the President's plans for a second death tax will undoubtedly hit middle-class Americans.

While it is true that the President won't be raising income taxes on Americans making less than $400,000 a year, middle-class Americans will unquestionably bear a substantial part of the burden of his tax hikes because raising taxes, any taxes, has consequences for everyone.

Democrats like to pretend that raising taxes is a consequence-free enterprise, but that isn't even close to being the truth. It doesn't take an economics degree to recognize that. It is common sense. Raise taxes enough on anyone or any business and that individual's behavior or that business's behavior is going to change. A business facing a substantial tax hike may raise prices; it may freeze salaries; or it may not hire as many new workers, and all of those decisions will be felt by ordinary Americans.

Think about it. If a business raises prices to deal with the impact of a tax hike, who is going to feel it the most? Ordinary Americans on a budget.

What is more, most Americans, if they are not self-employed or working for government, are employed by businesses, and if the business they work for isn't doing well, their prospects are going to be significantly affected. If businesses hold down wages to deal with the impact of tax hikes, for example, ordinary Americans' long-term earning potential will be diminished. These effects may not sound as concrete as being handed a tax bill, but they have just as real of an impact on Americans' incomes and Americans' lives.

Studies suggest that 50 to 70 percent or more of the burden of corporate tax hikes is borne by workers in the form of things like lower wages. Combine Democrats' proposed business tax hikes with their massive proposed increase in the capital gains tax, which would chill the investment that helps drive job creation, and you have a recipe for permanently diminished economic growth and a permanent reduction in opportunity for American workers.

If Democrats received any mandate in the last election, it was a mandate for moderation, for compromise, for bipartisan cooperation. Yet Democrats are behaving as if they had received a mandate for a partisan revolution. They are busy driving the country down the road to socialism with a massive and permanent expansion in the size of government, and their reckless tax-and-spending spree will hurt the very Americans they claim to want to help.

I hope some of my colleagues on the other side of the aisle will put the brakes on their party before the Democrats' massive spending spree ends in economic disaster for the American people.

I yield the floor.

The PRESIDING OFFICER. The Senator from Virginia.

CYBER INCIDENT NOTIFICATION ACT

Mr. WARNER. Mr. President, I rise in support of the Cyber Incident Notification Act of 2021.

I am very grateful to be joined by my colleague and friend, the senior Senator from Maine, because on this topic I am about to describe, she was way ahead of the curve, as she is on so many issues. She was so far ahead of the curve as to what we are talking about now, that if the Congress of the United States had adopted her proposals back in 2012—back in 2012—we might not be dealing with, literally, the catastrophic effects of cyber security incidents. We didn't, and that is why we are putting forward the Cyber Incident Notification Act of 2021.

It seems like, every day, Americans wake up to the news of another ransomware attack or cyber intrusion. The SolarWinds breach, which we learned about last December, resulted in the compromise of hundreds of Federal Agencies and private companies. The truth was, as we discovered, the bad guys actually got into 18,000 companies in the SolarWinds hack. Similarly, the ransomware attack on the Colonial Pipeline this past May resulted in gasoline and fuel shortages and price spikes across the entire eastern seaboard, demonstrating how broad

the ripple effects of these attacks can be.

The truth is these attacks can affect hundreds or even thousands of entities connected to the initial target. Earlier this week, the United States and allied governments publicly accused China's government of conducting an extensive hacking campaign on Microsoft's email systems, which again compromised tens of thousands of computers worldwide, including those used by some of the world's largest companies, contractors, and governments.

These events are finally the wake-up call that Senator COLLINS predicted a decade ago, a wake-up call for many of us in Washington, and even for those individuals who sit on these companies' boards that have to understand now the threats and capabilities possessed by our adversaries. These events also reveal major gaps in our Nation's effort to combat and contain cyber threats with insufficient communication between the private and public sectors.

These attacks and hacks demonstrate that our IT and critical infrastructure—much of it operated, appropriately, by the private sector—are under constant daily attack. They also demonstrate that we need to get better insight into cyber incidents as they happen—mid-incident—so that the U.S. Government can bring to bear its most effective capabilities and respond rapidly to protect our critical infrastructure systems.

We saw that recently when the FBI and the Department of Justice were able to claw back some of the ransomware from the Colonial Pipeline attack. With the Colonial Pipeline, what happened was we had a responsible private sector company that notified the government, FireEye, but we cannot rely upon the good will of private entities to individually, case by case, decide whether they tell the government. We need quicker and more comprehensive notification. In a sense, when an entity is being attacked, if that sector is being attacked, we can then notify other companies in that sector in realtime.

The truth is we should have done this much earlier. In fact, SolarWinds showed us that, when it comes to widescale breaches of U.S. networks, nobody is responsible for collecting information on the scope and scale of these attacks. This is alarming because this information allows us to develop a full picture of what was targeted and taken, what was at risk, and the type of techniques and tactics used by our adversaries.

These are all issues of critical national security, but as Senator COLLINS knows, under current law, there is no Federal mandate that companies disclose when they have been breached, even if they operate critical infrastructure. Rather, there is the hodgepodge of guidelines, depending on the industry, which, as we have seen, at least some companies then use as an excuse not to report or literally to create a whole set of legal gymnastics to avoid any level of disclosure. Unfortunately, this leaves our Nation vulnerable to criminal and state-sponsored hacking activity.

The bottom line is we cannot just rely on voluntary reporting to protect our critical infrastructure. We need a routine reporting requirement so that vital sectors of our economy that are affected by a cyber breach can have the full resources of the Federal Government and so that the private sector can be mobilized to respond to and fight off these attacks.

That is why I have been very proud to work not only with Senator COLLINS but also the vice chair of the Intelligence Committee, Senator RUBIO, and, in total, 15 of our colleagues, bipartisan, mostly all from the Intel Committee but also the chairman of the Defense Appropriations Committee and the chairman—on SASC—of the Cyber Committee, to introduce legislation this week that would require Federal Agencies, government contractors, and the owners and operators of critical infrastructure to report cyber intrusions within 24 hours of their discovery.

The purpose of this legislation is to ensure that the Federal Government is aware of and can take immediate action to mitigate cyber intrusions that have the impact to affect our national security. Part of that notification will be not just to let the government know but to let others in the private sector know as well. Consequently, the bipartisan Cybersecurity Incident Notification Act of 2021 would require covered entities to notify the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, or CISA, when a breach is detected so that the U.S. Government can mobilize to protect critical industries across our country. These covered entities include healthcare, transportation, financial services, agriculture, energy, and information technology sectors.

Now, the executive branch should have the flexibility to respond to shifting threats. The bill leaves some discretion for this and future administrations to determine whether other entities or classes of entities should be included at a later date.

To incentivize this information sharing to take place, the bill would grant limited immunity and confidentiality to companies that come forward to report a breach. It would also include data protection procedures to anonymize personally identifiable information and to, again, safeguard privacy.

These are not liability protections that would shield network operators, though, from negligence or misconduct. Rather, they would help prevent companies that come forward under this legislation from facing reputational risk just for reporting this vital information to the government.

Ultimately, I see this kind of notification as providing value, as I said, to the private sector as well so that we may have this common defense. There is no way we can solve this problem with government alone or with the private sector alone. There should not only be a rapid public notification but, in appropriate cases, swift government action.

Ultimately, we need to recognize that the threat landscape has fundamentally changed from even a few years ago. A few years ago, Senator COLLINS had this approach, and I think the private sector was concerned about undue mandates. The world has changed, and even many of the business organizations now agree that, as long as we grant that limited immunity and confidentiality, we need to put this reporting mechanism in place so that the public sector and the private sector can respond.

The truth is there are literally terabytes of sensitive data out there, including intellectual property, personal information, contract details, and others that could be exploited. For that matter, what if the SolarWinds attack had not been one of exploiting and taking out information but had actually been a denial-of-service attack, which we saw with Russia taking place against Ukraine a number of years back? That could have taken place with SolarWinds and completely shut down our economy, and we have all seen recently a dramatic upsurge in ransomware.

The truth is every company and virtually every part of government is under daily attack from these cyber criminals and, in some cases, from foreign intelligence services. The Federal Government must have the expertise and the willingness to share this information in realtime to make sure that we can counter this. I think this is a sensible first step in finally putting in place the kind of broad-based cyber strategy our country needs. So I urge my colleagues to join the 15 of us and pass the Cyber Incident Notification Act of 2021.

Again, I note my friend, the Senator from Maine, is here. We have been spending a lot of time together, but I really appreciate her lead sponsorship of this legislation.

I will say it on the floor of the Senate, as I have said in so many private settings over the last number of weeks on some other things, if we had just listened earlier to the Senator from Maine, we would have been in a lot better shape today in this country.

With that, I yield to my colleague, the Senator from Maine.

The PRESIDING OFFICER. The Senator from Maine.

Ms. COLLINS. Mr. President, first, let me thank my good friend and the leader of the Senate Intelligence Committee, Chairman WARNER, for paving the way for this legislation. He cares deeply about our country's response to these terrible cyber attacks and intrusions, and I am so grateful for his leadership and for his working with me to

produce the Cyber Incident Notification Act of 2021.

As the chairman has mentioned, this is a bipartisan bill that is broadly supported. It would strengthen our response to cyber attacks and, thus, help to prevent future cyber intrusions. It would require government Agencies, Federal contractors, and critical infrastructure entities, which are overwhelmingly owned and operated by the private sector and other important sectors, to notify the U.S. Government if they become the victims of a significant cyber attack or intrusion.

This effort is a direct outgrowth of our work on the Senate Intelligence Committee and reflects our longstanding concern regarding the lack of timely notification of cyber attacks that can lead to extremely serious consequences for our economy, for our national security, and for our individual privacy.

In September of 2019, for example, Russian hackers gained access to the SolarWinds' software. This resulted in a supply chain compromise that was downloaded by up to 18,000 of its customers. These hackers then conducted follow-on operations that compromised 9 Federal Agencies and 100 private-sector networks.

We did not become aware of this hack until more than a year later and only then because a cybersecurity firm called FireEye voluntarily notified the Federal Government and the public.

Just to reiterate that important point, FireEye was under no legal obligation whatsoever to tell us that the software had been compromised, even though it affected nine Federal Agencies. We are grateful that FireEye told us about this hack, but the fact that companies are not mandated to do so leaves our economy and national security vulnerable to future attacks and lessens our ability to respond effectively when such intrusions do occur.

Where would we be right now if FireEye had not voluntarily disclosed the intrusion? Would the Russians' operation still be ongoing? How much sooner would we have become aware of these Russian cyber operations if key sectors were required to report cyber incidents to the U.S. Government?

As the Senator from Virginia very kindly and generously noted, I have long been concerned about this problem and focused on it.

In 2012, when I was the ranking member of the Senate Homeland Security Committee, I joined with my chairman and dear friend former Senator Joe Lieberman of Connecticut in introducing a bill called the Cybersecurity Act of 2012. That bill would have, among other things, addressed this gap in cyber incident reporting. Unfortunately, our bill did not become law. How much more prepared we would be today if it had been enacted.

My 2012 bill would have led to improved information sharing between the private sector and the Federal Government that likely would have reduced the impact of cyber incidents on both the government and the private sector. Having a clear view of the dangers the Nation faces from cyber attacks is necessary to enable both the public and the private sector to mitigate and reduce the threat. We have just recently seen the impact of an attack on a major pipeline. Just think what the consequences would be of an attack that crippled our electric grid.

What we are proposing in the Cyber Incident Notification Act is common sense and long overdue. Our bill recognizes the additional burden that this reporting requirement places on parts of the private sector, and so it, therefore, provides additional liability protection for companies reporting cyber incidents and requires the government to harmonize these new mandates with any existing reporting requirements to help avoid duplication.

The bill also requires the government to produce analytic updates for the government and industry practitioners regularly so that they are aware of cyber incidents taking place and targeting their sectors. This should be a two-way street of the exchange of information.

Let us not delay any longer in passing a robust cyber incident notification requirement. Failure to pass this bill will only give our adversaries more opportunity to gather intelligence on our government, to steal intellectual property from our companies, to compromise our personal privacy, and, most of all, to harm our critical infrastructure.

Again, my thanks to the Senator from Virginia, the chairman of the Intelligence Committee, for his hard work on this bill. Let's get the job done.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. BARRASSO. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. SCHATZ). Without objection, it is so ordered.

NOMINATION OF TRACY STONE-MANNING

Mr. BARRASSO. Mr. President, I come to the floor today to oppose the nomination of Tracy Stone-Manning to be the Director of the Bureau of Land Management.

This morning, the Senate Energy and Natural Resources Committee voted on her nomination. Every Republican on the committee voted no. Before our business meeting was over, Senator SCHUMER came to this floor, to that desk, and he praised this nominee to the skies. President Biden and the Democrats have wrapped their arms around this nomination, and they won't let go.

So the question is, Who is this nominee whom the Democrats are embracing and every Republican voted against? Well, Tracy Stone-Manning is a graduate student who collaborated with ecoterrorists. Now, these are people who hammered hundreds of metal spikes—500 pounds of metal spikes—into trees in our national forest in Idaho. This is the kind of metal spike that they used—10 inches long, very thick; 500 pounds of these into the national forest.

Tree spiking involves nailing, hammering these rods into a tree. What happened? Why did they do that? Well, they want to stop progress in terms of logging. They want to stop progress in terms of firefighting. Because if a logger or a firefighter were to hit this rod with a chain saw, the chain saw would shatter. Devastating injuries have occurred as a result. If the saws used in timber mills or sawmills were to hit one of these as they are planing through the tree to produce boards, the entire blade shatters. It has been described to me by someone who has worked in one of these mills—it is like a hand grenade going off, damaging people all around in the vicinity. Well, the results can be fatal, and there are examples around the country where this has actually happened. Now, even the Washington Post has labeled tree spiking as ecoterrorism.

Tracy Stone-Manning, as a member of a radical group, edited, typed, and then anonymously sent a profanity-laced letter threatening the U.S. Forest Service. Here are just a few quotes from the letter.

She typed:

> You bastards go in there anyway and a lot of people could get hurt.

She typed:

> I would be more than willing to pay you a dollar for the sale, but you would have to find me first and that could be your WORST nightmare.

This is the letter she typed to the U.S. Forest Service. She then mailed this threatening letter to the target of the tree spiking, and the target was the U.S. Forest Service.

She and her circle were investigated. They were investigated for their involvement with this ring of ecoterrorists and this ecoterrorist attack that actually occurred to the U.S. forest. She was subpoenaed. She was ordered to give hair sampling, palm sampling, handwriting sampling, and fingerprint samples to the investigators.

She knew full well who the tree spikers were, and she could have easily gone to the authorities to identify them. She didn't. She covered it up for 4 years. She refused to cooperate with investigators.

Recently, within the last couple of months, Tracy Stone-Manning came before the Senate Committee on Energy and Natural Resources. She came for her confirmation hearing. Since that hearing and the statements that she made to the committee and affidavit she swore under oath and signed,